Washington, D.C. - Representatives Melissa Bean (IL-8), Artur Davis (AL-7) and Barney Frank (MA-4) have introduced H.R. 3140 to provide tough consumer protections and enforcement against credit card fraud and identity theft. The "Consumer Data Security and Notification Act of 2005," will strengthen federal protections against improper collection and sale of sensitive consumer information and provide consumers with advance warning when their personal financial information is at risk. In addition, the bill contains strong enforcement provisions to protect consumers from identity theft.

"Identity theft can be a horribly ironic nightmare for those who are financially responsible, live within their means and pay their bills on time - only to discover that a criminal has fraudulently used their identity to steal from them and destroy their credit rating for personal gain. As the number of identity theft incidents continues to rise, it is essential for Congress and business to work together to better ensure that consumers' private financial information is secure and that the companies holding that information are also adequately protected," Bean said.

"Congress needs to strengthen federal standards to provide more rigorous safeguards against the rising problem of identity theft. This bill represents a commonsense approach that rewards the legitimate expectations of consumers and the financial service industry," said Davis.

"Congress needs to enact tough enforcement measures to protect consumers from identity theft," said Congressman Frank, ranking minority member of the House Financial Services Committee. "The recent high profile accounts of data security breaches and possible criminal activity by hackers make the case that Congress needs to act soon with strong enforcement and accountability."

Recent high-profile data security breaches have undermined public confidence in the data security practices of many U.S. companies and exposed millions of consumers to potential fraud and identity theft. The theft of thousands of consumer files from companies like MasterCard, ChoicePoint and LexisNexis illustrates how broadly our private information is being collected and sold without our knowledge or consent and how vulnerable these private databases are to both traditional and high-tech forms of theft. Even consumers who have kept tight control of the personal and financial information could still become victims of identity theft if the companies that seek to profit from their personal information have inadequate security standards.

Original cosponsors for H.R. 3140 include committee Reps. Ackerman, Clay, Crowley, Davis, Ford, Frank, Gutierrez, Lynch, Maloney, McCarthy, Gwen Moore, Wasserman-Schultz, and Watt.

The Consumer Data Security and Notification Act of 2005 would make the following changes to federal law to enhance data security and help consumers protect their private information:

• Regulation of Data Brokers: Expands the Fair Credit Reporting Act (FCRA) to cover unregulated data brokers, such as ChoicePoint and LexisNexis, requiring them to operate by the same information sharing standards and consumer protections as consumer reporting agencies.

• New Data Security Standards: Imposes similar data security obligations and standards on data brokers and consumer reporting agencies as the Gramm-Leach-Bliley Act requires of regulated financial institutions.

• Uniform Data Breach Notification: Establishes uniform requirements for data brokers, consumer reporting agencies and financial institutions to notify consumers following a breach in any data system in which sensitive consumer information has been obtained by an unauthorized party and is likely to be misused.

• Notification by Merchants: Imposes greater responsibility on retail merchants to protect their customer's payment account information by requiring that any business that routinely collects and maintains customer credit card, checking or other payment information must notify customers or their financial institutions when financial account information has been obtained and is likely to be misused by unauthorized parties.

- - -

Detailed Summary to the Consumer Data Security and Notification Act:

A. Amendments to the Fair Credit Reporting Act (Title VI of the Consumer Credit Protection Act, 15 U.S.C. 1681 et seq.):

1. Include Data Brokers Under FCRA: Amends the definition of "consumer report" in section 603(d) to include any information communicated by a person or entity that regularly engages in the practice of assembling or evaluating personally identifiable information for the purpose of furnishing reports to third parties that include any of the following information relating to an individual: social security account number; driver's license number or other State identification number; bank or investment account number, credit card or debit card account number; and any password, access code, or security code relating to an account number or credit or debit card account number.

2. Verification of Users of Consumer Reports: Amends section 604(f) to prohibit a consumer reporting agency from providing a consumer report unless the identity of the person requesting the consumer report has been verified in accordance with procedures which the Federal Trade Commission shall prescribe in regulation.

3. Data Security Requirements: Adds a new section 630 to require the Federal Trade Commission to issue regulations extending the data security obligation and data protection standards of section 501 of Title V of the Gramm-Leach-Bliley Act to all consumer reporting agencies and data brokers.

4. Notification of Security Breaches: Adds a new requirement in section 630 that the Federal Trade Commission issue regulations requiring consumer reporting agencies and data brokers to provide written notification to any consumer upon becoming aware of unauthorized access to sensitive personal information relating to the consumer, unless, after appropriate investigation, the agency or broker can reasonably conclude that misuse of the information is unlikely to occur. The notice must include information relating to: the date of the security breach, the specific information or accounts acquired and a toll-free telephone number for obtaining additional information about the security breach and options for protecting the consumer's data files.

5. Treatment of Encrypted Information: Creates a reasonable assumption that misuse of information obtained in a security breach is unlikely, and notification is not required, where the

information has been encrypted according to standards identified by regulation.

6. Private Investigators: Clarifies that Licensed Private Investigators, which had previously obtained consumer information from data brokers for investigations unrelated to credit, insurance or employment, may obtain consumer reports under FCRA for legitimate investigations (including court actions, missing persons, locating heirs or beneficiaries, etc.), within the scope of their license, and for no other purpose.

7. Regulations: Directs the Federal Trade Commission to promulgate final rules implementing the changes made by the bill within 6 months of the date of enactment.

B. Amendments to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.):

1. Notification of Security Breaches: Adds an new subsection to the data security standards in section 501 requiring the financial regulatory agencies and the FTC to issue joint regulations requiring financial institutions to notify customers of data security breaches. The notice requirement would exceed the recent joint regulator notification rules by requiring a financial institution to provide written notification to any customer upon becoming aware of unauthorized access to sensitive personal information relating to the customer unless, after appropriate investigation, they reasonably conclude that misuse of the information is unlikely to occur and take reasonable steps to remedy the breach and safeguard the interests of affected customers. The notice must identify the date of the breach, the specific information or accounts believed to have been accessed in the breach, and provide a toll-free telephone number for obtaining additional information.

2. Required Notification by Retailers: Expands the definition of “financial institution” for purposes of the security breach notification requirement to include any person or entity that, in the regular course of business, collects and maintains written or electronic files containing payment information on customer transactions, including any bank account, credit card, debit card and any other payment account number. The entity responsible for the data base that was breached would be required to notify, as appropriate, the consumer, the consumer’s financial institution, or the financial intermediary that processed the debit or credit card transactions. A financial intermediary would be required to provide the financial institution issuing a credit card or holding the consumer’s account with all relevant information about the breach.

3. Treatment of Encrypted Information: Creates a reasonable assumption that misuse of information obtained in a security breach is unlikely, and notification is not required, where the information has been encrypted according to standards identified by regulation.

4. Regulations: Directs the federal financial regulators to issue joint regulations in final form to implement the changes made by the amendments within 6.

###